DEPARTMENT OF THE NAVY
NAVY ENVIRONMENTAL HEALTH CENTER
2510 WALMER AVENUE
NORFOLK, VIRGINIA 23513-2617

NAVENVIRHLTHCENINST 5510.1D
AS
29 MAR 2001

NAVENVIRHLTHCEN INSTRUCTION 5510.1D

Subj: INFORMATION AND PERSONNEL SECURITY PROGRAMS

Ref: (a) DOD 5200.1-R
(b) DOD 5200.2-R
(c) SECNAVINST 5510.30A
(d) SECNAVINST 5510.36
(e) OPNAVINST 5239.1B
(f) NAVENVIRHLTHCENINST 5239.1D
(g) SECNAVINST 5212.5D

Encl: (1) Emergency Plan

1. Purpose. To issue policy and revised procedures for the Navy Environmental Health Center (NAVENVIRHLTHCEN) Information Security and Personnel Security Programs.

2. Cancellation. NAVENVIRHLTHCENINST 5510.1C

3. Scope. The policy and procedures described herein are applicable to all NAVENVIRHLTHCEN personnel. Field activities are responsible for developing and maintaining programs.

4. Objective. To make sure of maximum uniformity and effectiveness of current Department of Defense (DOD) and Department of the Navy (DON) Information Security and Personnel Security policies by NAVENVIRHLTHCEN.

5. Basic Policy. The Information Security Program and the Personnel Security Program will ensure compliance with references (a) through (d) and make sure information classified under authority of Executive Order 12356 of April 2, 1982 is protected from unauthorized disclosure, and that the appointment or retention of civilian employees, acceptance or retention of military personnel, granting access to classified information, or assignment to other sensitive duties is clearly consistent with the interests of national security. No one will be granted knowledge, possession, or access to classified information because of rank, position or level of security clearance. Access to classified information will be controlled on a "need to know" basis.

6. Responsibilities.

a. Commanding Officer. The Commanding Officer is responsible for effectively carrying out the Information Security Program (ISP) and the Personnel Security Program (PSP) within the

command. He has overall responsibility for safeguarding all classified information and instructing personnel in security practices and procedures. The Commanding Officer is the ultimate authority for granting security clearances and is responsible for setting up a program for continuous evaluation of eligibility for access to classified information. The Commanding Officer is also responsible for evaluating the security posture of field activities. Reviews of field activities ISP and PSP will be conducted during regularly scheduled command inspections.

b. Command Security Manager. The Command Security Manager is appointed, in writing, by the Commanding Officer. He or she is the primary contact for information and personnel security in the command and is responsible to the Commanding Officer for managing the program in accordance with references (c) and (d). The Security Manager must be an officer or civilian employee, GS-11 or above, with enough authority and staff to manage the program. He or she must be a U.S. citizen and have been the subject of a favorably completed Background Investigation (BI).

c. Top Secret Control Officer (TSCO). When the Commanding Officer deems it necessary, a TSCO will be appointed, in writing. The TSCO is responsible to the Security Manager (if not the same person) for the receipt, custody, accounting for and disposition of Top Secret material in the command. The TSCO must be an officer, senior noncommissioned officer (E-7, E-8, or E-9) or civilian employee, GS-7 or above, and must be a U.S. citizen with a final Top Secret clearance. NAVENVIRHLTHCEN does NOT have the facilities for handling and storing Top Secret materials.

d. Assistant Security Manager. The Assistant Security Manager is appointed, in writing, and, except for issuing security clearances, helps the Security Manager in administering the Information and Personnel Security Program. He or she must be a U.S. citizen and either an officer, enlisted person E-6 or above, or civilian employee GS-6 or above. The investigative and clearance requirements for the Assistant Security Manager depend on the level of access to classified information needed. Assistant security managers must have an SSBI if they are designated to issue interim security clearances.

e. Security Assistants. Civilian and military member employees performing administrative functions under the direction of the security manager may be assigned without regard to rate or grade as long as they have the clearance needed for the access required to perform their assigned duties and taskings.

f. Information Systems Security Manager (ISSM). The ISSM is appointed, in writing, and acts as the focal point for all ADP security matters. The ISSM is responsible to the Security Manager for the protection of classified information being processed in the ADP systems (computers) and to the Physical Security Officer for the protection of personnel, equipment and related resources. Only specific computers will be used for preparing classified material. Detailed guidance about ADP security is available in references (e) and (f).

h. All Hands. Effective security is critical to national defense and completing the mission of this command and the Navy. Everyone is responsible for exercising sound security practices and procedures, and for following Information and Personnel Security Program regulations.

7. Security Education.

a. The purpose of the security education program is to make sure all personnel know how to protect and safeguard classified material. Some security education must be given to everyone, whether or not they have access to classified information. More extensive education must be given to those who do have access.

b. Following are the minimum requirements for security education:

(1) Indoctrination in basic security principles when entering the DON.

(2) Orientation of those who will have access to classified information at the time of assignment.

(3) On-the-job training in specific requirements for the duties assigned.

(4) Annual refresher briefings for those who have access to classified information.

(5) Counterespionage briefings once every two years for those who have access to information classified Secret or above.

(6) Special briefings as circumstances dictate.

(7) Debriefing at the time a Security Termination Statement, OPNAV Form 5511/14, is prepared.

8. Security Investigations. No one will be granted a clearance, given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made of his or her loyalty, reliability and trustworthiness. The first determination will be based on the minimum personnel security investigation (PSI) for the level of clearance needed. Before starting a PSI, the Security Manager will first make sure a valid investigation has not already been completed, and that locally available records (personnel, medical, legal, security, base police and other command records) do not have information which shows the person is not a good candidate for a position of trust. When it is decided that a PSI is needed, the Security Manager or Assistant Security Manager will help the person in completing the forms required by reference (c). In certain cases involving civilian employees, the Human Resource Office (HRO), will have already started a PSI. Satisfactory completion of a PSI will serve as the basis for granting a final security clearance. The PSI will be recorded in

Part II – Record of Investigation on the Certificate of Personnel Security Investigation, Clearance and Access, OPNAV Form 5520/20.

9. Security Clearance and Access.

a. Interim Clearance. An interim clearance for the level of access needed may be granted pending completion of full investigative requirements and pending establishment of a final security clearance by the Department of Navy Central Adjudication Facility (DON CAF). The review of local civilian law enforcement records, or the National Crime Information Center (NCIC), is prohibited. A check of the local Naval Investigative Service is not appropriate. The interim clearance may not be continued in excess of 1 year without a current confirmation from the DON CAF that the investigation contains no disqualifying information.

b. Final Clearance. When the results of a PSI are received, the Commanding Officer or Security Manager may grant a final clearance for the level of access needed to perform assigned duties. Security clearances will be recorded in Part III - Record of Clearance of OPNAV Form 5520/20. When a clearance is denied, the Security/Assistant Security Manager will enter "DENIED" in Part III and explain in the Comments section. The explanation, signed by the Commanding Officer or Security Manager, will not specify the cause for denial, but will refer to the personnel record entry, command correspondence or other documentation supporting the action.

c. Access. The Commanding Officer or Security Manager may grant access to classified information to people who have an official need-to-know and a valid security clearance. The Security Manager is responsible for continuously evaluating eligibility for access to classified information. Each command may use a method of record maintenance suited to the command's capabilities, such as a computerized database, a log book, or a form OPNAV 5520/20, and must maintain the record for 2 years after access terminates. The command access record must include the following data elements: Name, SSN, citizenship verification, date and level of access authorized, the basis of the access determination and the name and title, rank or grade of the individual authorizing the access. Interim security clearance is recorded on the OPNAV 5510/413. Access is automatically terminated when the person transfers from the command, is discharged or is separated from Federal Service. When a clearance is administratively withdrawn, or revoked, for cause, the access based on the clearance is cancelled.

d. Adjustment/Termination of Clearance and Access:

(1) When there is no longer a need for access to a particular level of classified material, the clearance will be administratively lowered or withdrawn. When a clearance is withdrawn, the Security/Assistant Security Manager will overwrite the clearance entry with, "WITHDRAWN," in Part III of OPNAV Form 5520/20, and the Comments section must be annotated to show the action was taken administratively, with no prejudice to the individual's future eligibility for access to classified material. Adjust access to reflect current need.

(2) When a clearance is revoked for cause, the Security/Assistant Security Manager will overwrite the clearance entry with, "REVOKED," in Part III of OPNAV 5520/20, and explain in the Comments section. The explanation, signed by the Commanding Officer or Security Manager, will not specify the cause for revocation, but will refer to the personnel record entry, command correspondence or other documentation supporting the action.

(3) When the clearance and access have been reduced or terminated, the person will be debriefed in accordance with reference (c).

(4) Reinvestigations to update a previous investigation must be conducted in accordance with reference (c). Periodic Reinvestigations (PRs) are conducted on personnel whose clearance/access to Top Secret information is based on an investigation that is 5 years old or more. Secret Periodic Investigations (SPRs) are required for persons with a Secret clearance at 10-year intervals. Confidential Periodic Reinvestigations (CPRs) are required for persons with a Confidential clearance at 15-year intervals.

(5) Reciprocal acceptance of security clearances eliminates the need to revalidate security clearances by DON CAF when military or civilian personnel become assigned to NAVENVIRHLTHCEN. Review of records that show prior clearance will be sufficient to grant clearance and access at the gaining activity.

10. Receipt, Handling and Storage of Classified Material.

a. All classified material received at NAVENVIRHLTHCEN during normal working hours will be turned over to a security clerk in the Correspondence Control Division for recording and storage. Classified material received after normal working hours will be retained in the personal custody of the individual receiving the material until the material can be turned over to the security manager, or an authorized security assistant. A log entry on the receipt of classified material will be made. Security container combinations will not be given out over the phone for any reason. At the first opportunity, the classified material will be turned over to a security assistant for proper recording and storage. When transferring classified material, a log entry will be made, and will be initialed by the receiving security assistant.

b. All classified material will be handled in strict compliance with reference (d). Persons reviewing or hand carrying classified information or material will take every precaution to prevent unauthorized disclosure. When this is done within the command, as part of normal duties, it will be kept in a file folder with a classified information cover sheet, and will be kept in the responsible person's physical custody at all times. When the person is finished with the classified material, it will be returned to the Correspondence Control Division for storage. When classified material is transported outside the command (such as to and from the message center), it will be double wrapped (in a file folder, inside a brief case), and will always be kept in

the responsible person's physical possession.

c. People who generate classified material are responsible for the information security of all working papers, including scrap paper, notes, drafts, etc. These items will not be thrown in the trash. Working papers, typewriter ribbons and computer disks used in preparing classified material will be given the same protection needed for the highest level of classification they were used to create and, therefore, need to be secured in a command security container. Classified material will not be prepared nor stored on unclassified hard disk drives. All classified documents, including working papers, will be given to the Security Manager or Assistant Security Manager for classification review. Classified messages can only be prepared on AIS with removable hard drive.

d. Copying classified material will only be done with approval of the Security Manager, and using only designated copying machines. Two people will be involved in copying classified material to make sure of positive control and safeguarding of classified material, that only authorized copies are made and the number of copies is kept to a minimum. A sign will be posted by these machines that reads: "THIS MACHINE MAY BE USED FOR REPRODUCTION OF MATERIAL UP TO SECRET. REPRODUCTION MUST BE APPROVED BY THE COMMAND SECURITY MANAGER." After copying classified material, several copies of unclassified material will be made to make sure latent images of the classified information are not left in the equipment or on other material. Machines that are not authorized for copying classified material will be posted with a warning notice that reads: "THIS MACHINE IS LIMITED TO REPRODUCTION OF UNCLASSIFIED MATERIAL ONLY."

11. Telephone Security. Discussing, transmitting or "talking around" classified information over the telephone is prohibited, except as may be authorized on approved secure communication circuits. DOD telephones are subject to communications security monitoring at all times and are provided for the transmission of official government business only.

12. Disposal and Destruction.

a. The Security Manager is responsible for the periodic review, destruction and disposal of classified material. The method used to destroy classified material must prevent later recognition or reconstruction. Classified material will be destroyed as soon as it is no longer needed and will not be kept for more than five years from the date of origin unless authorized by reference (g).

b. Classified material will be destroyed only by authorized means by staff personnel cleared to the level of the material being destroyed. Classified material and "burn bags" will be safeguarded at the level of the highest classification of the information they contain until they are completely destroyed.

c. A record of destruction is required for Top Secret information. Records of destruction are not required for Secret and Confidential information except for special types of classified information as defined in reference (d).

13. Visit Control.

a. General visiting will be allowed on an unclassified basis only, and the movement of all visitors throughout NAVENVIRHLTHCEN will be restricted to protect classified information. A visitor is any person who is not attached to nor employed by NAVENVIRHLTHCEN, including persons on temporary additional duty (TAD).

b. When a visit to NAVENVIRHLTHCEN will involve access to classified information, the commanding officer of the visitor or an official of the contractor facility, organization or foreign country which the visitor represents will send a Visit Request, OPNAV Form 5521/27, or similar letter or message request, to the Commanding Officer, NAVENVIRHLTHCEN. Formal visit requests are not needed for personnel of the Executive Branch of the Government who are U.S. citizens or immigrant aliens with whom working relationships have been established.

14. Audits. The Security Manager and Assistant Security Manager will, at a minimum, conduct an annual audit of the classified material kept at NAVENVIRHLTHCEN. This audit may be held in conjunction with the periodic review and destruction of classified material. The Classified Material Log kept by Correspondence Control Division will be verified and annotated as to the current inventory of classified material.

15. Emergency Plan. Enclosure (1) gives the requirements for carrying out the emergency plan for the protection of classified material in case of natural disaster, civil disturbance or enemy action.

16. Review Responsibility. The Security Manager is responsible for the periodic review and update of this instruction.

D. M. SACK

Distribution: (NAVENVIRHLTHCENINST 5215.2P
List V (All NAVENVIRHLTHCEN Personnel)
VI (NAVENPVNTMEDU's)
VII (NAVDISVECTECOLCONCEN's)
VIII (NAVENVIRHLTHCEN DET)
IX (NAVDRUGLAB's)

EMERGENCY PLAN

1. The Emergency Plan will normally be executed at the direction of the Commanding Officer, an authorized representative, or by higher authority.

2. There are three basic kinds of emergency where the use of this plan may be needed. The action to be taken will be basically the same for each, with certain changes to meet particular situations. They are:

a. Natural disaster, such as fire, flood, hurricane or earthquake.

b. Civil disturbance or uprising.

c. Enemy action.

3. There are three courses of action for safeguarding classified material. They are (in order of desirability):

a. Secure Material. Before leaving spaces where classified material is located, the person having custody will make sure the material is securely stowed in an authorized security container.

b. Remove Material. Classified material will be removed from the normal storage area and kept in the custody of the person(s) evacuating the area. The material will be safeguarded either until returned to the building or until other safe storage areas can be identified.

c. Destroy Material. Destroy classified material in the following order:

(1) Top Secret.

(2) Secret.

(3) Confidential.

d. Get a trash can and take the material from the safe in the above order. Under normal circumstances there should be no Top Secret material stored at NAVENVIRHLTHCEN. Take the material to the loading dock at the rear of the building and destroy it by burning. Keep a Classified Material Control Log as evidence of any Top Secret material destroyed.

4. Destruction, loss, or compromise of any classified material will be reported immediately to the Security Manager, who will brief the Commanding Officer and prepare the necessary reports.

5. Classified Material will be inventoried as soon as possible after the emergency.